UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/672,811	09/26/2003	Tom Thuan Cheung	SVL920030076US1	8922

28342 7590 12/19/2006

SAMUEL A. KASSATLY LAW OFFICE
20690 VIEW OAKS WAY
SAN JOSE, CA 95120

EXAMINER	
SHAN, APRIL YING	
ART UNIT	**PAPER NUMBER**
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/19/2006	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/672,811	CHEUNG, TOM THUAN	
	Examiner	Art Unit	
	April Y. Shan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 September 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 September 2003* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/26/2003*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20 have been examined.

Drawings

2. The drawings are objected to under 37 CFR 1.83(a). The drawings fig. 1A- 5B must show every feature of the invention specified in the claims. Therefore, the encrypting the original string using the derivative equations and the factors must be shown or the feature(s) canceled from the claim(s). No new matter should be entered.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

3. Claims 1-17 and 19-20 are objected to because of the following informalities:

a. For claim 1, "defining an encryption equation that transforms....and that genertate...". The sentence structure is grammatically incomprehensible and the second "that" is misleading. Please remove the second "that".

b. For claims 2, 3, 16-17 and 19-20 the sentence structure in the first part of the claims is grammatically incomprehensible. For purposes of examination and based on the Applicant's specification, the claims are interpreted to read that "wherein the set of factors comprises at least one of....";

c. For claim 7, the sentence structure is grammatically incomprehensible. Please rewrite.

d. For claim 8, the sentence structure is grammatically incomprehensible. Please rewrite.

e. For claim 15, "implementor" should be "implementer" because according to the Applicant's specification, e.g. [0041], it was spelled as "implementer". For the purpose of consistency, please correct.

Any claim not specifically addressed, above, is being objected as incorporating the deficiencies of a claim upon which it depends.

Please check the claims and correct any informality the Applicant is aware of. Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 1-20 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

As per claims 1-20, as based on a disclosure, which is not enabling. The steps of identifying/building relationships between the encryption equation and a set of derivative equations and how the derivative equations and the factors encrypt the original string is critical or essential to the practice of the invention, but not included in the claim(s) and not enabled by the disclosure. See *In re Mayhew*, 527 F.2d 1229, 188 USPQ 356 (CCPA 1976)

Also, the claim limitation of "defining an encryption equation ... and that generates corresponding derivatives" is not enabling. According to block 415 in fig. 4 of the present application, it discloses, "encryption module generates factors and derivatives", not "encryption equation generates corresponding derivatives". Please see paragraph [0048] of the present application, it discloses, "The encryption module 210 generates factors 220 as required by the encryption module 210 and calculates derivatives". Additionally, the claim limitation of "encrypting the original string using the derivative equations and the factors" is not enabling. Please see block 425 in fig. 4 of the present

application, it discloses, "encrypt character using encryption equation", not "encrypting the original string using the derivative equations and the factors". Further, in paragraph [0035]-[0036] of the present application, "the encryption equation maps a character in the original string to a character in the encrypted string". From the specification, one of ordinary skill in the art will conclude that the encryption module generates corresponding derivatives and the encryption equation performs the task of encrypting the original string, not the derivative equations and the factors. In re Wands, *858 F.2d 731, 737, 8 USPQ2d 1400, 1404 (Fed. Cir. 1998)*. In claim 1, the Applicant already defined an encryption equation to transform the original string to an encrypted string, then later in claim 1, encrypting the original string using the derivative equations and the factors? Did the Applicant mean multiple encryptions on the original string using first encryption equation and then the derivative equations and the factors? If so, it was not disclosed in the claims and based on the disclosure, which is not enabling.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> **Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.**

7. Claims 1-20 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1-14 are directed to a method for encrypting an original string. The examiner respectfully asserts that the claimed subject matter does not fall within the statutory classes listed in 35 USC 101. The claimed steps do not result in a tangible

result. Claims 1-14 are rejected as being directed to an abstract idea (i.e., producing non-tangible result) [tangible requirement does require that the claim must recite more than a 101 judicial exception, in that the process must set forth a practical application of that 101 judicial exception to produce a real-world result, Benson, 409 U.S. at 71-72, 175 USPQ at 676-77).

Claims 15-17 are directed a system for encrypting and decrypting an original string. However, it appears that the system to one of ordinary skill in the art is software, per se. There is no element positively recited as part of the system. Applicant's specification on page 7, paragraph [0023] provides no explicit and deliberate definition on any element positively recited as part of the system, and it appears that such would reasonably be interpreted as representative of the software which encrypts and decrypts an original string. As such, it believed that the system of claim 15-17 is reasonably interpreted as functional descriptive material, per se.

Claims 18-20 are directed a computer program product for encrypting and decrypting an original string. It appears to one of ordinary skill in the art that the computer program product is software, per se. As such, it believed that the computer program product of claims 18-20 is functional descriptive material, per se.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claims 1-10 and 12-20 are rejected under 35 U.S.C. 102(b) as being anticipated by Blakley, III et al. (U.S. Patent No. 5,677,952).

As per **claim 1**, Blakley, III et al. discloses a method of encrypting (abstract) an original string ("data (i.e., a string x)" – e.g. col. 5, lines 10-11), comprising:

selectively defining a set of factors ("a password Pu and possibly a user name and other usercheck data" – e.g. col. 5, lines 43-44. Please note a password Pu and possibly a user name and other usercheck data corresponds to Applicant's factors) that represents factors to be used for encrypting the original string (abstract);

defining an encryption equation ("encryption function 86, usually an XOR" – e.g. col. 5, lines 39-40, col. 6, line 10) that transforms the original string to an encrypted string (col. 5, lines 39-40) and generates corresponding derivatives ("the secret key is derived from a password entered into the computer by an authorized user" and "an index" – e.g. abstract. Please note secret key and index corresponds to Applicant's derivatives);

selectively defining a set of derivative equations ("pseudorandom function 84" – e.g. col. 5, line 38. Please note pseudorandom function corresponds to Applicant's derivative equation) that represents relationships between the factors and the derivatives to introduce a predetermined degree of randomness in encrypting the original string (abstract); and

encrypting the original string using the derivative equations and the factors (col. 5, lines 39-40, col. 6, lines 4-11).

As per **claim 2**, Blakley, III et al. discloses a method as applied above in claim 1. Blakley, III et al. further discloses wherein the set of factors comprises any one or more of: constant values, numbers, objects, and random values that are derived from events ("a password Pu and possibly a user name and other usercheck data" – e.g. col. 5, lines 43-44).

As per **claim 3**, Blakley, III et al. discloses a method as applied above in claim 1. Blakley, III et al. further discloses wherein the set of factors comprises any one or more of: constant values, numbers, objects, and random values that are derived from values provided by equations ("a password Pu and possibly a user name and other usercheck data" – e.g. col. 5, lines 43-44.)

As per **claim 4**, Blakley, III et al. discloses a method as applied above in claim 1. Blakley, III et al. further discloses wherein the derivative equations comprise mathematical functions that are defined in terms of the factors ("a= SHA(Pu)+Ku" – e.g. col. 5, lines 3-9)

As per **claim 5**, Blakley, III et al. discloses a method as applied above in claim 1. Blakley, III et al. further discloses wherein the number of the derivative equations is at

least equal to the number of the factors ("a length-increasing pseudorandom function and a password" – e.g. abstract).

As per **claim 6**, Blakley, III et al. discloses a method as applied above in claim 1. Blakley, III et al. further discloses wherein the original string is comprised of characters (("data (i.e., a string x)" – e.g. col. 5, lines 10-11. To a person with ordinary skill in the art at the time of the invention, a string is composed of a sequence of characters representing human-readable text. Therefore, Blakley, III et al. met the claim limitation by disclosing a string X).

As per **claim 7**, Blakley, III et al. discloses a method as applied above in claim 1. Blakley, III et al. further discloses wherein the encryption equation comprises a mathematical function of a character of the original string and of the factors (e.g. abstract and col. 5, lines 39-40, col. 6, lines 9-10).

As per **claim 8**, Blakley, III et al. discloses a method as applied above in claim 1. Blakley, III et al. further discloses comprising determining factor decryption equations for mapping the derivatives to a plurality of mapped factors (col. 6, lines 25-47).

As per **claim 9**, Blakley, III et al. discloses a method as applied above in claim 8. Blakley, III et al. further discloses comprising determining a decryption equation as a mathematical function of an encrypted string in the encrypted string and the plurality of

mapped factors (col. 6, lines 25-47).

As per **claim 10**, Blakley, III et al. discloses a method as applied above in claim 9. Blakley, III et al. further discloses comprising storing the encrypted string in a database with a set of stored derivatives (col. 6, lines 25-33 and lines 48-57).

As per **claim 12**, Blakley, III et al. discloses a method as applied above in claim 1. Blakley, III et al. further discloses comprising decrypting the encrypted string based on the derivatives and the derivative equations (col. 6, lines 25-47).

As per **claim 13**, Blakley, III et al. discloses a method as applied above in claim 1. Blakley, III et al. further discloses wherein selectively defining the set of factors comprises defining at least one factor ("a password Pu and possibly a user name and other usercheck data" – e.g. col. 5, lines 43-44.)

As per **claim 14**, Blakley, III et al. discloses a method as applied above in claim 1. Blakley, III et al. further discloses wherein selectively defining the set of derivative equations comprises defining at least one derivative equation (abstract).

As per **claim 15**, Blakley, III et al. discloses a system for encrypting and decrypting (abstract) an original string ("data (i.e., a string x)" – e.g. col. 5, lines 10-11), comprising:

an implementor ("an authorized user" – e.g. abstract. Please note an authorizied user corresponds to an implementor) selectively defines a set of factors ("a password Pu and possibly a user name and other usercheck data" – e.g. col. 5, lines 43-44. Please note a password Pu and possibly a user name and other usercheck data corresponds to Applicant's factors) that represents factors to be used for encrypting the original string (abstract);

the implementor further defines an encryption equation ("encryption function 86, usually an XOR" – e.g. col. 5, lines 39-40) that transforms the original string to an encrypted string (col. 5, lines 39-40) and that generates corresponding derivatives ("the secret key is derived from a password entered into the computer by an authorized user" and "an index" – e.g. abstract. Please note secret key and index corresponds to Applicant's derivatives);

the implementor further selectively defines a set of derivative equations ("pseudorandom function 84" – e.g. col. 5, line 38. Please note pseudorandom function corresponds to Applicant's derivative equation) that represents relationships between the factors and the derivatives to introduce a predetermined degree of randomness in encrypting the original string (abstract);

and an encryption module encrypts the original string using the derivative equations and the factors (col. 5, lines 39-40).

As per **claim 16**, Blakley, III et al. discloses a system as applied above in claim 15. Blakley, III et al. further discloses wherein the set of factors comprises any one or

more of: constant values, numbers, objects, and random values that are derived from events ("a password Pu and possibly a user name and other usercheck data" – e.g. col. 5, lines 43-44).

As per **claim 17**, Blakley, III et al. discloses a system as applied above in claim 15. Blakley, III et al. further discloses wherein the set of factors comprises any one or more of: constant values, numbers, objects, and random values that are derived from values provided by equations ("a password Pu and possibly a user name and other usercheck data" – e.g. col. 5, lines 43-44).

As per **claims 18-20**, Blakley, III et al. discloses the claimed method of steps as applied above in claim 1-3. Therefore, Blakley, III et al. discloses the claimed computer program product having instruction codes for carrying out the method of steps.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

12. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Blakley, III et al.

As per **claim 11**, Blakley III et al. discloses a method of encrypting an original string as applied above and further discloses any other information (e.g. the secret key) useful in encrypting and decrypting is stored in the memory and the ciphertext and Fa(i) may be combined in some other way to determine x. (col. 6, lines 36-37 and line 50). And a one-way function of the secret key a is installed to distinguish correct and incorrect passwords (col. 5, line 61- col. 6, line 2. Please note the derivatives of incorrect passwords corresponds to Applicant's false derivatives).

Blakely III et al. did not expressly disclose the limitation a plurality of false derivatives will not be used to decrypt the encrypted string.

It would have been obvious to a person of ordinary skill in the art at the time of the invention that "combined in some other way to determine x" as taught in Blakley III et al. as only use the correct derivates from correct password to decrypt the encrypted string. The motivation is doing so would be "to protect the confidentiality of information stored on a storage device of a computer, even if the computer is stolen or otherwise access without the owner's consent or knowledge", as taught by Blakley, III et al. (col. 1, lines 44-47)

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-892)

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to April Y. Shan whose telephone number is (571) 270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AYS

8 December 2006
AYS

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100